

REMARKS

Claims 1, 60, 61, 63-65, 68, 69, 73 and 76-78 have been amended and new claim 79 has been added. Accordingly, claims 1, 57-69, and 71-79 are pending in this patent application. Reconsideration of the rejections in view of the remarks below is requested.

Applicant firmly believes the application is in condition for allowance. If the Examiner does not believe so, Applicant kindly requests the Examiner to contact Applicant to arrange an interview so that the claimed subject matter can be discussed with respect to Williams to conserve USPTO resources and maximize remaining available patent term.

Claims 63-69 and 71-78 were rejected under 35 U.S.C. §101 as allegedly being directed to non-statutory subject matter. The rejection is respectfully traversed.

Without agreeing or acceding to the merits and propriety of this rejection, and solely to expedite prosecution, claims 63 and 68 have been amended to recite a computer program product, embodied in a non-transitory computer-readable storage media.

Accordingly, Applicant requests withdrawal of the rejection under 35 U.S.C. §101.

Claims 1, 57-61, 63-69, 71, 73, 74 and 76-78 stand rejected under 35 U.S.C. §102(e) as being anticipated by United States patent no. 5,815,657 to Williams et al. ("Williams"). The rejection is respectfully traversed.

As discussed, for example, at pages 6-8 of Applicant's specification, Applicant has recognized that a person relying on a digital certificate of a counterparty to a transaction has no effective recourse should the certificate be invalid, inauthentic, etc. For example, the person has no effective recourse against the counterparty – after all, it is the counterparty that is providing the invalid, inauthentic, etc. certificate. Further, the person has no effective recourse against a certificate authority that issued the certificate because there is no relationship between the person and the certification authority with respect to the counterparty's certificate.

Applicant has discovered a solution to this issue. In general terms, the solution as described in claim 1 involves a particularized method by which a first party can obtain a transactional financial assurance and recourse (e.g., a guarantee) with respect to particular electronic infrastructure used in or with a transaction involving a second party in a situation

where there is electronic assurance with respect to the second party but the first party isn't able to properly rely on that electronic assurance.

As an example embodiment disclosed in the application, a certification authority may issue a primary certificate (e.g., subscriber assurance of an attribute and an example of electronic infrastructure used in or with a transaction involving the subscriber) with respect to a subscriber. The subscriber forms a transaction and then provides the transaction to a relying party, the transaction including the primary certificate issued by the certification authority or an identification of that certificate. The relying party evaluates the transaction sent by the subscriber and determines whether transaction financial assurance on, for example, the authenticity of the primary certificate is needed in order to "safely" proceed with the transaction. If the relying party determines that assurance is needed, it sends to the reliance server a request for assurance with respect to the primary certificate, e.g., whether the primary certificate is authentic. Then the reliance server determines whether or not to provide the requested assurance. The reliance server bases its determination on the primary certificate. Based on its determination, the reliance server issues to the relying party a secondary certificate providing the assurance to the relying party. See, e.g., page 10, line 21 to page 11, line 20. Thus, in this way, the relying party has effective recourse with respect, for example, an inauthentic primary certificate when otherwise it would not.

In view of the foregoing, Applicant respectfully submits that the cited portions of Williams are directed to entirely different technology and do not teach claim 1. For example, Applicant respectfully submits that the cited portions of Williams fail to disclose, *inter alia*, obtaining electronic signals representing a request for transactional financial assurance and recourse, the transaction financial assurance and recourse being with respect to-electronic infrastructure used in or with a transaction involving the subscriber, and the transactional financial assurance being other than a digital signature of the electronic infrastructure or the electronic signals representing subscriber assurance, the request including a value of the transaction financial assurance and recourse requested; determining whether to provide the requested transactional financial assurance and recourse based on at least the subscriber assurance and whether the requested transaction financial assurance value exceeds a reliance limit associated with the electronic signals representing subscriber assurance; and, depending on the determining, issuing electronic signals representing the requested transactional financial assurance and recourse to a relying party hardware mechanism; and tracking cumulative liability associated with the electronic signals representing subscriber assurance, wherein

determining whether the requested transaction financial assurance value exceeds the reliance limit includes determining whether the requested transaction financial assurance value causes the cumulative liability to exceed an acceptable reliance limit in excess of the reliance limit, as recited in claim 1.

Rather, the cited portions of Williams appear to merely describe an electronic monetary system that provides for transactions utilizing an electronic-monetary system that emulates a wallet, a purse, a smart card, a pocketbook, a checkbook, a satchel or other payment instrument holder that is customarily used for storing money, credit cards and other payment instruments. Access to the wallet is restricted by a password. When access is authorized, a graphical representation (bitmap) of the instrument(s) is presented on the display based on either a user default, an instrument issuer default or payment instrument holder default to enable a user to select a payment instrument for use in a particular transaction. Once a payment instrument is selected, a summary of the goods for purchase are presented to the user and the user enters their electronic approval for the transaction or cancels the transaction. Electronic approval results in the generation of an electronic transaction to complete the order. See, e.g., Williams, col. 2, line 56 to col. 3, line 8.

So, for example, the cited portions of Williams appear to be silent as to transaction financial assurance and recourse with respect to electronic infrastructure used in or with a transaction involving the subscriber. While the Williams system includes various components of electronic infrastructure, there appears to be nothing in the cited portions of Williams about its system giving any sort of assurance and recourse (e.g., guarantee) with respect to any part of the electronic infrastructure (e.g., that it is authentic, valid, accurate, etc.). The cited portions of Williams system appear to describe a conduit for money transfer for transactions but appear not to provide any assurance or recourse.

The Office Action has referred to certificates and digital signatures in Williams. However, it appears that the certificates in the cited portions of Williams appear merely to occupy their traditional role as described above and in Applicant's specification and thus have the shortcomings identified by Applicant. For example, a merchant has no effective recourse with respect to a customer's certificate and similarly, a customer has no effective recourse with respect to a merchant's certificate. For similar reasons, a digital signature by the customer or by the merchant is ineffective; a digital signature is merely a mathematical scheme to give a recipient a reason to believe that a message was created by a known sender but can easily be invalid, inauthentic, etc. like a certificate.

To avoid any misunderstanding, Applicant has specified in claim 1 that the recited transactional financial assurance and recourse is not a digital signature of the electronic infrastructure or the electronic signals representing subscriber assurance (e.g., a customer certificate). Accordingly, the X.509 certificates referenced in col. 11, lines 31-38 of Williams are excluded as being the transactional financial assurance and recourse. In stark contrast, it is precisely such certificates that suffer from the problems described above and for which claim 1 provides a solution.

The Office Action states that the "types of certificates taught by Williams are not mere public key certificates or mere digital signatures. For example The X.509 type certificate was designed to allow the certificate to convey a great deal more information than a mere public key certificate. Such a certificate has many extensions and fields, and is commonly known in the art as capable of conveying financial transaction information among other types." However, even if the certificate identified in col. 11, lines 31-38 of Williams is capable of conveying various information, it is not the recited transactional financial assurance and recourse. For example, it is specifically excluded from claim 1 since that certificate is electronic signals representing subscriber assurance (i.e., a certificate as to certain consumer attributes). Moreover, even if it were assurance and recourse (which Applicant does not concede), it would be with respect to consumer or merchant attributes. There is nothing about it representing assurance and recourse with respect to electronic infrastructure used in or with a transaction. In other words, the consumer certificate is in respect of consumer personal information, such as identity, but not about a consumer's electronic infrastructure (e.g., a consumer certificate).

Further, Applicant submits that the cited portions of Williams appear to be silent regarding a value of a transaction financial assurance and recourse requested and then determining whether to provide the requested transactional financial assurance based on whether the requested transaction financial assurance value exceeds or is below a reliance limit associated with the electronic signals representing subscriber assurance, as recited in claim 1. There appears to be nothing in the cited portions of Williams regarding the recited value in a request or determining whether the recited value exceeds or is below the recited reliance limit. Applicant notes that language similar to that from allowable claim 62 has been incorporated into claim 1.

Further, Applicant submits that the cited portions of Williams appear to be silent regarding tracking cumulative liability associated with the electronic signals representing

subscriber assurance, wherein determining whether the requested transaction financial assurance value exceeds or is below the reliance limit includes determining whether the requested transaction financial assurance value causes the cumulative liability to exceed or be below an acceptable reliance limit in excess of the reliance limit, as recited in claim 1. Not only does there not appear to be anything in the cited portions of Williams regarding the recited reliance limit, there further appears to be nothing in the cited portions of Williams regarding the recited cumulative liability tracking or determining whether the recited value exceeds or is below an acceptable reliance limit in excess of the reliance limit.

Claims 57-61 and 76 depend from claim 1 and are, therefore, patentable for at least the same reasons provided above related to claim 1, and for the additional features recited therein.

For many of the same reasons as provided above, Applicant respectfully submits that the cited portions of Williams fail to disclose a computer program product, embodied in a computer-readable media, comprising instructions for causing a computer to effect a method of managing reliance in an electronic transaction system as recited in claim 63. For example, Applicant submits that the cited portions of Williams fail to disclose causing electronic signals representing the reliance request message to be sent to a reliance server requesting a transactional financial assurance and recourse for the aspect of the transaction upon which the relying party intends to rely, the transactional financial assurance and recourse including transactional financial assurance and recourse with respect to electronic infrastructure used in or with the transaction and the transactional financial assurance and recourse being other than a digital signature of the electronic infrastructure, the request including a value of the requested transaction financial assurance and recourse for comparison with a reliance limit associated with the aspect of the transaction, as recited in claim 63.

Claims 64-67 and 77 are patentable by virtue of their dependency, and for the additional features recited therein.

For many of the same reasons as provided above, Applicant respectfully submits that the cited portions of Williams fail to disclose a computer program product, embodied in a computer-readable media, comprising instructions for causing a computer to effect a method of managing reliance in an electronic transaction system as recited in claim 68. For example, Applicant submits that the cited portions of Williams fail to disclose receiving electronic signals representing a reliance request message, the message specifying an aspect of a transaction upon which a relying party intends to rely, requesting assurance for the aspect of

the transaction, and including a value of the assurance requested, and determining whether to provide transactional financial assurance and recourse with respect to electronic infrastructure used in or with the transaction based on the reliance request message and whether the value of the assurance exceeds or is below a reliance limit associated with the aspect of the transaction, the transactional financial assurance and recourse being other than a digital signature of the electronic infrastructure, as recited in claim 68.

Claims 69, 71, 73, 74 and 78 are patentable by virtue of their dependency, and for the additional features recited therein.

Accordingly, Applicant respectfully requests that the rejection under 35 U.S.C. §102(e) of claims 1, 57-61, 63-69, 71, 73, 74 and 76-78 based on Williams be withdrawn and the claims be allowed.

New claims 79 is patentable over the applied reference by virtue of its dependency, and for the additional features recited therein.

All rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance. If questions relating to patentability remain, the examiner is invited to contact the undersigned to discuss them.

Should any fees be due, please charge them to our deposit account no. 03-3975, under our order no. 061047/0268225. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced deposit account.

Respectfully submitted,
MILLSBURY WINTHROP SHAW PITTMAN LLP

Jean-Paul Hoffman
Reg. No. 42,663
Tel. No. 703-770-7794
Fax No. 703-770-7901

February 28, 2011
P. O. Box 10500
McLean, VA 22102
(703) 770-7900